VZCZCXYZ0005
PP RUEHWEB

DE RUEHUL #1098/01 1910720
ZNY CCCCC ZZH
P 100720Z JUL 09
FM AMEMBASSY SEOUL
TO RUEHC/SECSTATE WASHDC PRIORITY 4989
INFO RUEHBJ/AMEMBASSY BEIJING 6270
RUEHMO/AMEMBASSY MOSCOW 0007
RUEHKO/AMEMBASSY TOKYO 6360
RUEHIN/AIT TAIPEI 3692
RHHMUNA/CDR USPACOM HONOLULU HI
RUALSFJ/COMUSJAPAN YOKOTA AB JA
RUACAAA/COMUSKOREA INTEL SEOUL KOR
RHMFISS/COMUSKOREA J5 SEOUL KOR
RHMFISS/COMUSKOREA SCJS SEOUL KOR
RHEHNSC/NSC WASHINGTON DC
RUEKJCS/SECDEF WASHINGTON DC//OSD/ISA/EAP//

C O N F I D E N T I A L SEOUL 001098

SIPDIS

E.O. 12958: DECL: 07/10/2019
TAGS: KS KN PGOV PREL
SUBJECT: CYBER ATTACKS: NIS PREMATURE IN BLAMING NORTH KOREA

Classified By: A/DCM Joseph Y. Yun. Reasons 1.4 (b,d).

¶1. (C) Summary: Reports by South Korea's National Intelligence Service (NIS), leaked by National Assembly lawmakers, that blamed North Korea for the recent spate of Denial of Service cyber attacks against U.S. and South Korean websites quickly fueled hysteria in South Korea's conservative print media. The inability of the NIS, however, to produce any evidence that North Korea or its "sympathizers" are behind the attacks has subsequently provoked criticism from progressive lawmakers, who accuse the government of purposely misleading the public about the source of the attacks. The incident reflects poorly on the NIS and, by extension, the Lee Myung-bak Administration, and risks lending credence to Pyongyang's claims that Seoul's hardline policy is the primary obstacle in continuing inter-Korean talks. END SUMMARY.

Background

¶2. (SBU) On July 8, the NIS briefed select lawmakers about the cyber attacks that had begun the previous day and disrupted service on South Korean government and private sector websites. These NIS briefings reported that North Korea or North Korean sympathizers may have been to blame for the attacks. The brief, provided both verbally and in documentary form, quickly leaked to the press, with lawmakers downplaying the NIS's uncertainty. South Korean media reports cited "intelligence officials" who said that, while technical proof was not yet available, North Korea was almost certainly behind the attacks. The articles also referenced Fox News and Associated Press reports citing unnamed Defense Department officials who made the same claims. Apparently, much of the NIS's case rested on previous North Korea hacking attacks and North Korea's June 27 threats about a "high-tech war" in response to Seoul's plan to participate in the U.S.-led exercise "Cyber Storm," which simulates a federal response to a major cyber attack.

Increasing Media Hysteria

¶3. (C) Immediately after the leak of the NIS brief -- at least one newspaper managed to get the entire document -- conservative media outlets quickly fanned the flames by releasing a series of reports representing North Korea's involvement as a foregone conclusion. The Joongang Daily --

one of Korea's big-three newspapers -- cited the CEO of an internet security company who compared the cyber attacks to the September 11, 2001 attacks in the United States. Another major newspaper, the Chosun Ilbo, ran a story today titled, "North Korea's Powerful Hacker Army," which describes cyber warriors who are believed to have declared war on the South in the late 1990s. In still another article, "a source familiar with intelligence matters" said that hacking attempts on South Korean military and USFK computer networks had increased 15 percent compared to 2008.

New doubts

¶4. (C) Today's inflammatory reports coincided with new doubts about the lack of tangible evidence linking North Korea to the attacks. Backtracking quickly, the NIS today said the attacks were traced to 86 internet protocol addresses in 16 countries, including South Korea, the United States, Japan, and China but not to North Korea. These reports, which government officials note does not rule out North Korean involvement, are raising doubts in South Korea and provoking criticism from opposition lawmakers. The Democratic Party spokesperson accused the NIS of trying to achieve political aims and speculated it might be seeking to build support for a pending bill that would increase the organization's funding and jurisdiction. The spokesperson also suggested that the NIS was trying to reinforce the hardline North Korean policy of the current administration.

Comment

¶5. (C) Blamed by the conservatives for overly accommodating the Sunshine Policy during the Roh Moo-hyun/Kim Dae-jung era, the NIS went through a major personnel reshuffle over the past six months. The NIS director, Won Sei-hoon, deputy mayor for political affairs when President Lee was Seoul Mayor, received a clear mandate from the Blue House to return the NIS to an intel and security agency, not a policy-making agency. Many critics have argued, even before the cyber attack incident, that the NIS was interpreting its new mandate to return to the bad old days of the KCIA, especially in dealings with North Korea. These critics now have another rallying cry, because there is an increasing public perception that the NIS overstated the threat for its own political gain. Among critics of the current government's policy toward North Korea, the misrepresentation of NIS claims is likely to give credence to North Korea's argument that the real cause for stalled inter-Korean talks -- especially the most recent talks over the Kaesong Industrial Complex (KIC) -- is South Korea's overly hardline policy toward the North.
STEPHENS